SecurityGen
Telecom Security. Transcending Generations.

Securing The Global 5G Growth Story with Network Functions Virtualisation Infrastructure (NFVi)

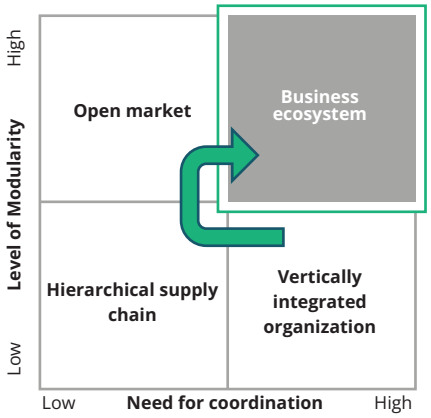
2020 became the year of 5G proliferation (as per Qualcomm study), while 2021 is about a rapid 5G rollout, vertical expansion, and advancing 5G systems with new capabilities. The same gets reflected in an August 2021 Gartner forecast that estimates 5G coverage in tier-1 cities across the US by 2024 will be 60%, besides predicting a revenue growth from $794 million to $1.6 billion in western Europe, by the year-end.

Spike in remote working due to the pandemic is a significant factor in this growth, with individual consumer and business demand for connectivity rising significantly.

The situation demands CSPs to look into hardware acceleration for boosting performance, considering scalability and reliability while maintaining a low latency level. Network Function Virtualisation (NFV) and cloud-based 5G rollout are the answers they resort to, transitioning from legacy network infrastructures. However, with increased bandwidth and unprotected IoT devices comes the risk of advanced threats and vulnerabilities. The critical question remains - "Is 5G secure under the NFV environment?". To answer this, let's dive deeper to understand legacy architecture and the transition from legacy networks to NVF.

From Legacy Vendor to the 'Ecosystems'

The Telecom industry has learned from several pitfalls across its almost 150 years of operational history, all valuable but few at high costs. Initially, one operator would likely produce most of its equipment, cables, tools, and shoulder responsibilities of training the technical personnel on its activities. Over time, the model evolved to a hierarchical supply chain - usually based on a single vendor providing all the necessary tools, solutions, and (proprietary technology) training. Even today, many Mobile Network Operators (MNOs) are still dependent on their primary vendor and have never left this model. Nevertheless, after many years of 3GPP's hard work on standardisation, some operators managed to evolve to an Open Market approach - a significant advance for the 4G environment. MNOs could finally get best-in-class solutions, despite their primary or legacy vendor providing a similar one. LTE-Advanced (aka 4G+) and 5G present a different challenge, proven as manageable by an even newer kind of business infrastructure: The Ecosystems.



Source: Jacobided et al (2018)

Ecosystems – Why do They Need a Virtualization

Ecosystem - a term borrowed from Biology generally refers to a group of interacting firms that depend on each other's activities. Rakuten, the many times studied Japanese MNO, has built its own based on about ten different vendors and over 100 different functions. Their model may now be used as a Cloud-based service for other MNOs. Whether the MNOs use third-party ecosystems or build their own, the supply chain complexity has increased, and its risk must be analysed and assessed after deployment. No single provider makes a complete 5G Network, mainly due to the

Cloud Native architecture, so the goal moves from best-in-class to best-in-breed. Telecom is finally embracing the de facto IT standard and not reinventing all hardware, data centre switching, virtualisation, virtual switching, orchestration, and performance components. The MNOs need to procure these from top performance vendors. MNOs have to manage components using VNF or CNF architectures over a shared infrastructure for the first time. Considering that the usual endpoint security tools such as EDRs and antivirus are not accepted for performance reasons, the architecture plays a huge role in the overall security level.

How To Keep The 5G Cloud Safe in This Ecosystem?

The truth is much of the recommendations are the basic ones, although the challenges are more significant:

Inventory management: In addition to knowing every application and information asset that exists, you must keep a consistent naming, classification, and categorisation policy also for the assets that may be created dynamically by an orchestrator.

• Use knowledge from inventory to keep resources, including containers, from being shared between functions with different security classifications or requirements

• For instance, the UDM contains centralised data on subscribers and private information such as their physical location and should not share resources or have connectivity at any level with a less secure third-party application such as a connection speed tester

Identity & Access management: Authorising human users using Multifactor Authentication is mandatory, but all entities - Functions, VMs, O&M Services, etc. – that access any resourc must also be authenticated and have its authorisation verified.

• Use Certificates for authentication of functions, especially in the 5G Core

• Segregate the Certification Authority from the virtual environment

• Certification infrastructure, deployment and lifecycle require special attention

Log Monitoring: Automated logging, monitoring, and analysis are vital. Telecom is all about availability, and usually, MNOs are focused on recovering service rather than keeping track of possible abuses or compromise of assets. Stakeholders must consider that cloud is here to provide additional availability and efficiently managing its security is a significant investment.

Segmentation: Segment networks as far as possible (including virtual ones). Everyone hates filling forms to request connectivity, and firewall rules must be created. Nevertheless, the same needs to be designed and well classified for each function or service, no matter how extensive or distributed the network.

Cloud is about scaling, integrating different sites and domains seamlessly, which eventually will include shared and public clouds. 'First time right' should be the motto when designing Telco Clouds.

Monitoring: Monitoring for lateral movement attempts and any traffic that doesn't fit the baseline or is characteristic of adversarial techniques execution is a must. That's a good practice and even more necessary if operators fail to keep up with the previous ones.

Above all, one must consider the complexity of the new supply chain and make sure to have clear and accurate:

1. Application validation: At least the NFVI software stack boot process must have a transparent chain of trust and assurance to avoid compromising the entire environment
2. Aggressive Security Patching Process
3. The onboarding process for new Functions and Updates
4. Vulnerability Management Process
5. Solution and Service Providers Risk Management Process

Reference:

1. **Towards a theory of ecosystems** - London Business School 2018 - Michael G. Jacobides | Carmelo Cennamo | Annabelle Gawer

2. **ENISA Documentation** https://www.enisa.europa.eu/publications/enisa-threatlandscape-report-for-5g-networks/

3. **CISA Documentation** https://www.cisa.gov/publication/5g-strategy

4. **3GPP on virtualization impacts:** 3GPP TR 33.848

About SecurityGen

Founded in 2022, SecurityGen is a global start-up focused on telecom security. We deliver a solid security foundation to drive secure telecom digital transformations and ensure next-gen enterprise intelligent connectivity.

Connect With Us

Email: **contact@secgen.com**
Website: **www.secgen.com**

UK | Italy | Czech Republic | Brazil | Mexico
India | South Korea | Japan | Malaysia